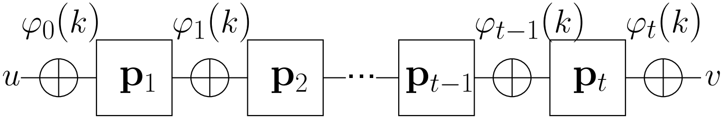
Chosen-Key Secure Even-Mansour Cipher from a Single Permutation

Shanjie Xu, Qi Da, Chun Guo

shanjie1997@mail.sdu.edu.cn, daqi@gmail.com, chun.guo@sdu.edu.cn
School of Cyber Science and Technology, Shandong University,
Qingdao, Shandong, China

Iterated Even-Mansour (IEM)



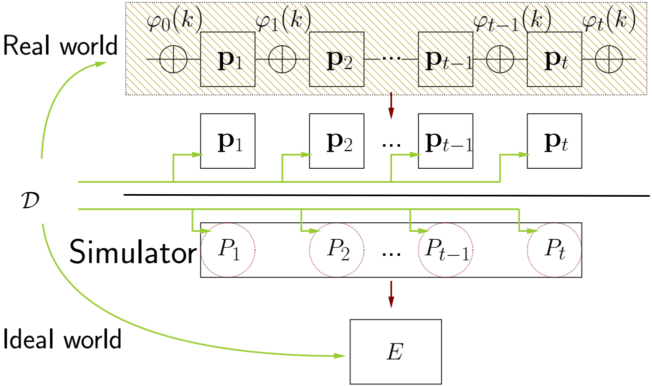
- *Key schedule* $\varphi_i : \{0,1\}^{\mathcal{K}} \to \{0,1\}^n$
- *Permutations* $\mathbf{p}_i : \{0,1\}^n \to \{0,1\}^n$

Iterated Even-Mansour (IEM)

- It abstracts *substitution-permutation network*.
  - PRESENT (ISO)
  - Skinny (ISO)
  - AES
- Modeling $\mathbf{p}_1, ..., \mathbf{p}_t$ as public random permutations, variants of this scheme provably achieve various security notions.

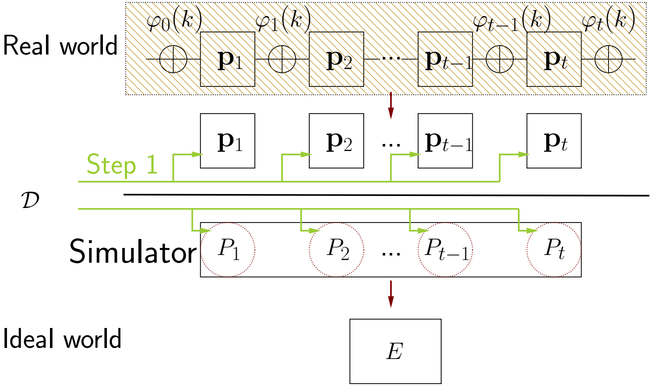
Indifferentiability

- The classical security definition for a blockcipher is indistinguishability from a secret random permutation.



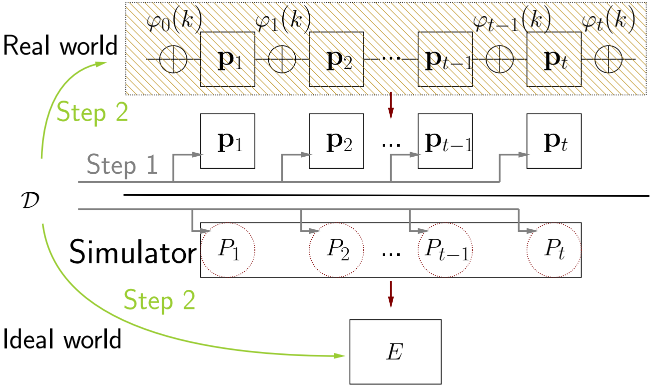
Sequential Indifferentiability

- Cogliati and Seurin[CS15] advocated the notion of sequential-indifferentiability.



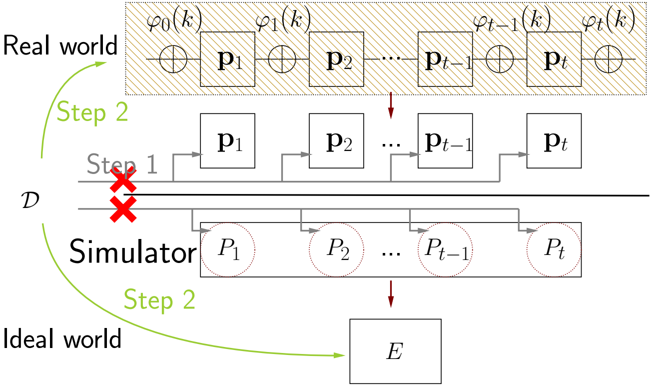
Sequential Indifferentiability

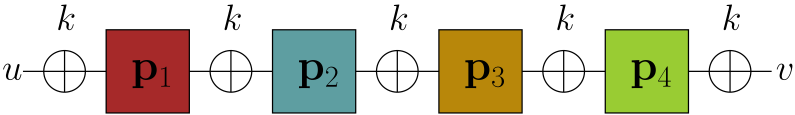
- Cogliati and Seurin[CS15] advocated the notion of sequential-indifferentiability.



Sequential Indifferentiability

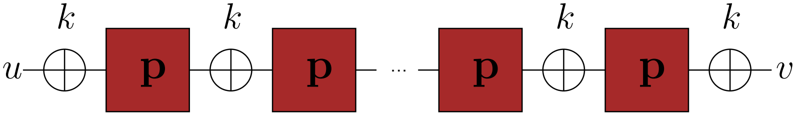
- Cogliati and Seurin[CS15] advocated the notion of sequential-indifferentiability.





- **Cogliati and Seurin's Work**
  The *"single-key" Even-Mansour* variant EMIP without any non-trivial key schedule is proved sequential indifferentiability at 4 rounds.
- **Our Question**
  Whether sequential indifferentiability is achievable using a single permutation?

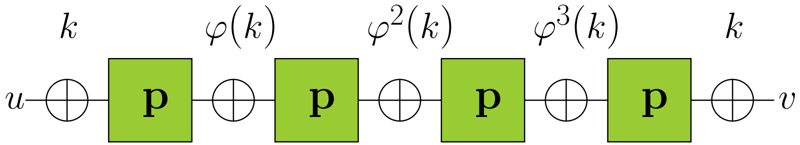
Attack[XDG23]



- Even in the weaker model of seq-indifferentiability, the *"single-key"*, *single-permutation Even-Mansour* variant EMSP remains insecure, regardless of the number of rounds.
  1. Query $y \leftarrow \mathbf{p}(x)$;
  2. Let $k = x \oplus y$;

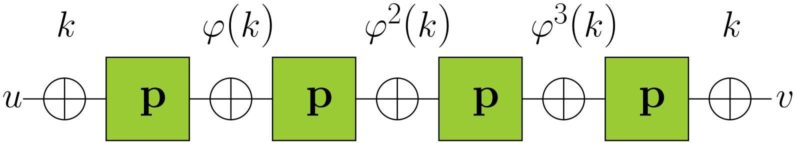
  $\Rightarrow$ $u = y$ and $v = x$.

Minimal and Secure Construction



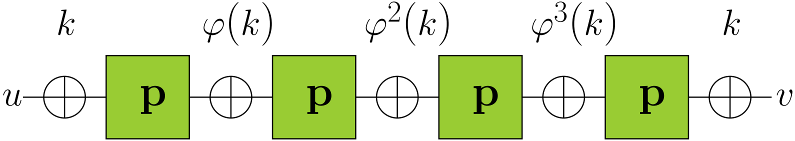
The minimal construction EMSP using a single random permutation $\mathbf{p} : \{0,1\}^n \to \{0,1\}^n$ and an affine key schedule permutation $\varphi : \{0,1\}^n \to \{0,1\}^n$. One can set φ to be a linear orthomorphism, or $\varphi(k) := k \ggg_a$.

Proof Approach



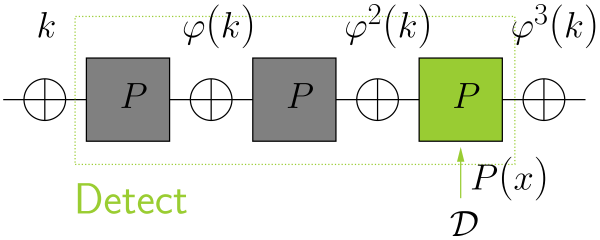
1. Construct a simulator that resists obvious attack.
2. It remains to argue:
   - The simulator is efficient, i.e., its complexity can be bounded;
   - The simulator gives rise to an ideal world that is indistinguishable from the real world.

Proof Approach



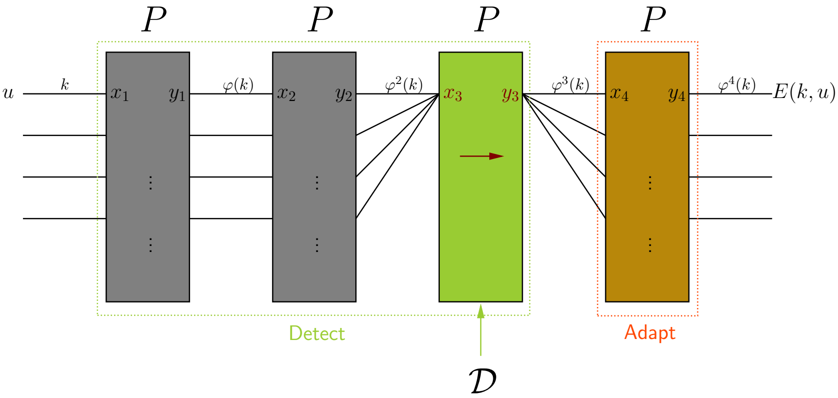
1. Chain complete technique;
2. Internal values are secret and random.

Simulator: 3-chain

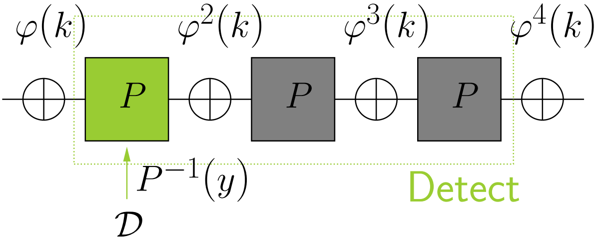


When D queries $P(x)$, the simulator first checks whether it can form a 3-chain.

Simulator: 3-chain

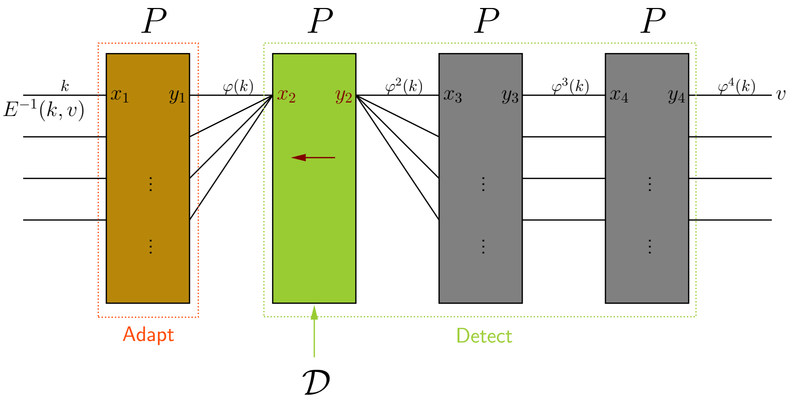


Simulator: 3-chain

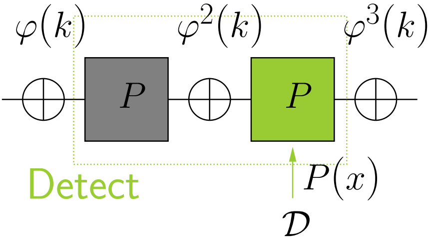


When D queries $P^{-1}(y)$, the simulator checks whether the 3-chain is formed in the opposite direction.

Simulator: 3-chain

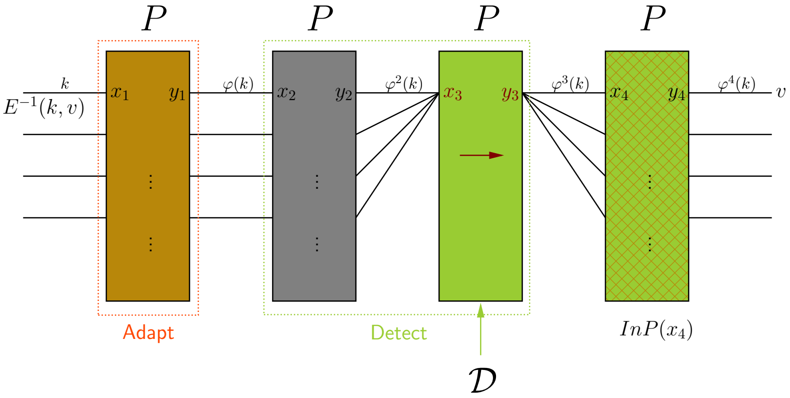


Simulator: 2-chain

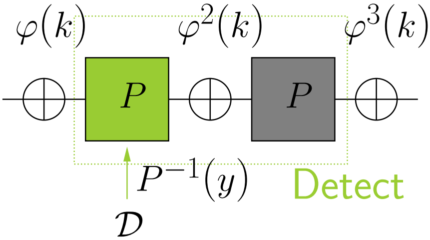


After completing the 3-chain check, the simulator also needs to check the 2-chain. When D queries $P(x)$, the simulator checks the 2-chain of the form as above.

Simulator: 2-chain

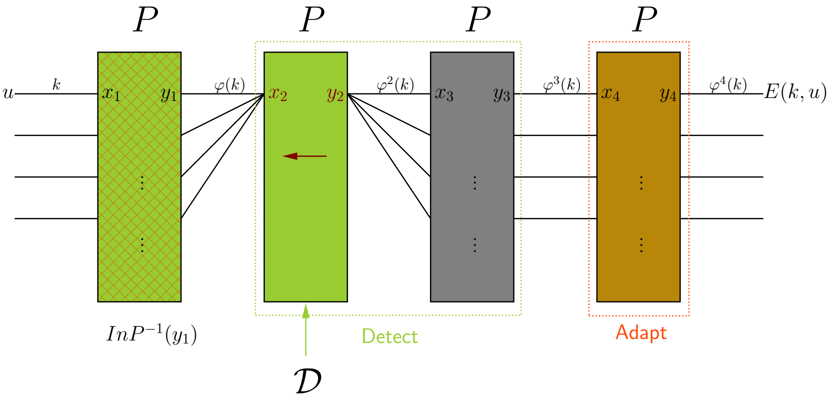


Simulator: 2-chain

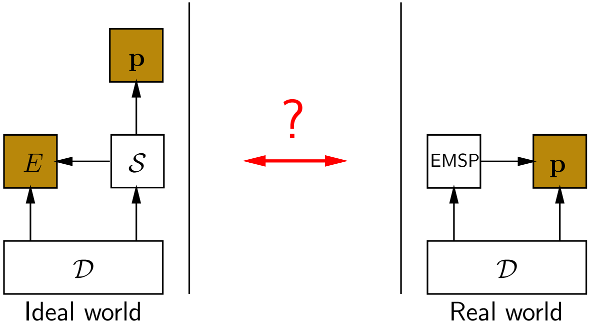


When D queries $P^{-1}(y)$, the simulator checks whether the 2-chain is formed in the opposite direction.

Simulator: 2-chain

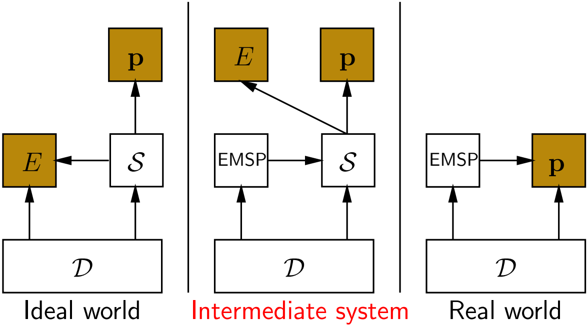


Security Bound



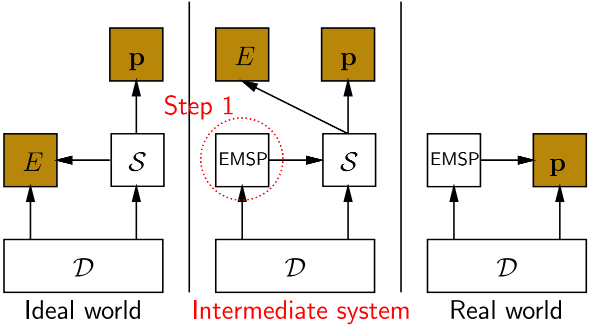
How to get distance between ideal world and real world?

Intermediate system



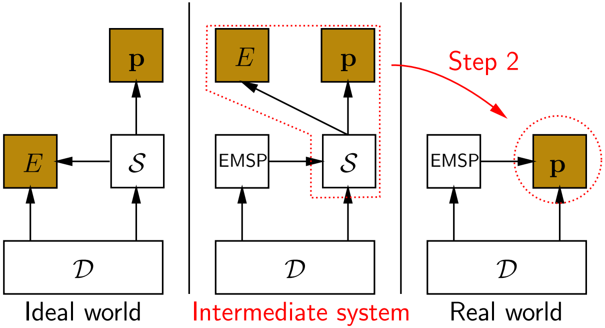
Getting distance between ideal world and real world can be divided into two steps:

Intermediate system



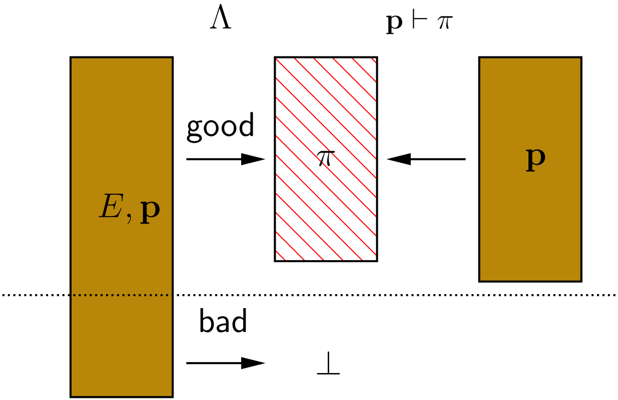
Step 1: $\Delta \leq \Pr[(E, \mathbf{p} \text{ is bad})]$.

Intermediate system



Step 2: Randomness mapping.

Randomness mapping



Comparison

Scheme	EMIP_4	EMKD_3	EM2P	$\mathsf{EMSP}_4[\varphi]$
Rounds	4	3	4	4
Primitives	4	4	2	**1**
Key sch.	no	random oracle	no	iterative
Complex.	q^2	q^2	q^2	q^2
Bounds	$q^4/2^n$	$q^4/2^n$	$q^4/2^n$	$C(\varphi)q^7/2^n$ $+q^{10}/2^n$
Ref.	[CS15]	[GL16b]	[XDG23]	this work

Thank you for listening!